Symantec Enterprise Security Manager™ Best Practice Policy Manual

ISO 17799 standard-based best practice policies for AIX operating systems

Best Practice Policy Manual for AIX

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

Copyright © 2001-2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Symantec Enterprise Security Manager, LiveUpdate, and Symantec Security Response are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

SYMANTEC CORPORATION SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "I DO AGREE" OR "YES" BUTTON OR LOADING THE PRODUCT, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON AND DO NOT USE THE SOFTWARE.

1. LICENSE TO USE

Licensor grants You a non-exclusive, non-transferable license (the "License") for the use of the number of licenses of Licensor's software in machine readable form, and accompanying documentation (the "Product"), on Your machines for which You have been granted a license key and for which You pay the License fee and applicable tax. The License governs any releases, revisions or enhancements to the Product that Licensor may furnish to You.

2. RESTRICTIONS

Product is copyrighted and contains proprietary information and trade secrets belonging to Licensor and/or its licensors. Title to Product and all copies thereof is retained by Licensor nd/or its licensors. You will not use Product for any purpose other than for Your own internal business purposes or make copies of the software, other than a single copy of the software in machine-readable format for back-up or archival purposes. You may make copies of the associated documentation for Your internal use only. You shall ensure that all proprietary rights notices on Product are reproduced and applied to any copies. You may not modify, decompile, disassemble, decrypt, extract, or otherwise reverse engineer Product, or create derivative works based upon all or part of Product. You may not transfer, lease, assign, make available for timesharing or sublicense Product, in whole or in part. No right, title or interest to any trademarks, service marks or trade names of Licensor or its licensors is granted by this License.

3. LIMITED WARRANTY

Licensor will replace, at no charge, defective media and product materials that are returned within 30 days of shipment. Licensor warrants, for a period of 30 days from the shipment date, that Product will perform in substantial compliance with the written materials accompanying the Product on that hardware and operating system software for which it was designed, as stated in the documentation. Use of Product with hardware and/or operating system software other than that for which it was designed and voids this applicable warranty. If, within 30 days of shipment, You report to Licensor that Product is not performing as described above, and Licensor is unable to correct it within 30 days of the date You report it, You may return Product, and Licensor will refund the License fee. If You promptly notify Licensor of an infringement claim based on an existing U.S. patent, copyright, trademark or trade secret, Licensor will indemnify You and hold You harmless against such claim, and shall control any defense or settlement. This warranty is null and void if You have modified Product, combined the Product with any software or portion thereof owned by any third party that is not specifically authorized or failed promptly to install any version of Product provided to You that is non-infringing. If commercially reasonable, Licensor will either obtain the right for You to use the Product or will modify Product to make it non-infringing. The remedies above are Your exclusive remedies for Licensor's breach of any warranty contained herein.

4. LIMITATION OF REMEDIES

THE WARRANTIES IN THIS AGREEMENT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OF ANY PRODUCT OR ITS DOCUMENTATION. THE LIABILITY OF LICENSOR HEREUNDER FROM ANY CAUSE OF ACTION WHATSOEVER WILL NOT EXCEED THE AGGREGATE LICENSE FEE PAID BY LICENSEE FOR THE PRODUCT. IN NO EVENT WILL LICENSOR OR ITS AUTHORIZED REPRESENTATIVES BE LIABLE FOR LOST PROFITS OR SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF, OR INABILITY TO USE, THE PRODUCT OR LOSS OF OR DAMAGE TO DATA, EVEN IF LICENSOR OR ITS AUTHORIZED REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LICENSOR AND ITS AUTHORIZED REPRESENTATIVES WILL NOT BE LIABLE FOR ANY SUCH CLAIMS BY ANY OTHER PARTY. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. No action or claim arising out of or relating to this Agreement may be brought by You more than one (1) year after the cause of action is first discovered.

5. CONFIDENTIALITY

You agree that Product and all information relating to the Product is confidential property of the Licensor ("Proprietary Information"). You will not use or disclose any Proprietary Information except to the extent You can document that any such Proprietary Information is in the public domain and generally available for use and disclosure by the general public without any charge or license. Use by persons to which You have contracted any of Your data processing services is permitted only if each contractor (and its associated employees) is subject to a valid written agreement prohibiting the reproduction or disclosure to third parties of software products and associated documentation to which they have access and such prohibitions apply to the Product. You recognize and agree that there is no adequate remedy at law for a breach of this Section, that such a breach would irreparably harm the Licensor and that the Licensor is entitled to equitable relief (including, without limitation, injunctive relief) with respect to any such breach or potential breach, in addition to any other remedies available at law.

6. EXPORT REGULATION

You agree to comply strictly with all US export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses to export, re-export or import Product. Export or re-export of Product to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

7. US GOVERNMENT RESTRICTED RIGHTS

If You are licensing Product or its accompanying documentation on behalf of the US Government, it is classified as "Commercial Computer Product" and "Commercial Computer Documentation" developed at private expense, contains confidential information and trade secrets of Licensor and its licensors, and is subject to "Restricted Rights" as that term is defined in the Federal Acquisition Regulations ("FARs"). Contractor/Manufacturer is: Symantec Corporation, and its subsidiaries, Cupertino, California, USA.

8. MISCELLANEOUS

This License is made under the laws of the State of California, USA, excluding the choice of law and conflict of law provisions. Product is shipped FOB origin. This License is the entire License between You and Licensor relating to Product and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communication between the parties during the term of this License. Notwithstanding the foregoing, some Products or products of Licensor may require Licensee to agree to additional terms through Licensor's on-line "click-wrap" license, and such terms shall supplement this Agreement. If any provision of this License is held invalid, all other provisions shall remain valid unless such validity would frustrate the purpose of this License, and this License shall be enforced to the full extent allowable under applicable law. Except for additional terms that may be required through Licensor's on-line "click-wrap" license, no modification to this License is binding, unless in writing and signed by a duly authorized representative of each party. The License granted hereunder shall terminate upon Your breach of any term herein and You shall cease use of and destroy all copies of Product. Duties of confidentiality, indemnification and the limitation of liability shall survive termination or expiration of this Agreement. Any Product purchased by You after the purchase of Product which is the subject of this License shall be subject to all of the terms of this License. All of Symantec Corporation's and its subsidiaries' licensors are direct and intended third-party beneficiaries of this License and may enforce it against You. Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). Licensee may obtain Content Updates for any period for which Licensee has purchased Upgrade Insurance for the Software, entered into a maintenance agreement with Symantec that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates.

Contents

Symantec ESM Best Practice Policy Manual for AIX

Introducing best practice policies 4
How best practice policies differ from ESM default policies 4
How base policies differ from high-level policies 5
Industry research sources 6
Installing best practice policies 7
Installation prerequisites 7
Installation steps 7
AIX base policy 9
OS Patches checks and templates 9
Password Strength checks 9
Startup Files checks and templates 10
AIX high-level policy 11
Account Integrity checks 11
File Attributes checks 12
File Find checks 13
File Watch checks 14
Login Parameters checks 14
Network Integrity checks 15
Password Strength checks 15
Startup Files checks 15
User Files checks 16
Known restrictions 17
Registration of new agents to ESM 5.1 managers 17

Service and support solutions

Before contacting technical support 19
Service and support Web site 21
Service and support offices 22

Symantec ESM Best Practice Policy Manual for AIX

This manual documents the ISO 17799 standard-based best practice policies for Symantec Enterprise Security Manager™ (ESM) agents on AIX operating systems. The documented policy is provided for ESM 5.1 and ESM 5.5 managers and agents that are running Security Update 9 or later module releases.

This chapter includes the following topics:

- Introducing best practice policies
- Installing best practice policies
- AIX base policy
- AIX high-level policy
- Known restrictions

Introducing best practice policies

ESM best practice policies are configured by members of the Symantec Security Response team to protect specific applications and/or operating system platforms from security vulnerabilities that could compromise the confidentiality, integrity, and/or availability of data that is stored and transmitted on your computer network.

Best practice policies are designed to enforce "common best practices" as described in the ISO/IEC 17799 international standard, "Information technology - Code of practice for information security management," and defined through research by trusted security experts and clearing houses.

Note: ESM best practice policies are based on sections of the ISO 17799 standard that address logical access controls and other security issues pertaining to electronic information systems. Symantec recommends that you review the ISO 17799 standard in its entirety to identify other issues, such as physical access controls and personnel training, that need to be addressed in your organization's information security policy.

How best practice policies differ from ESM default policies

The Phase 1, 2, and 3 default policies that are installed with ESM core product and Security Update releases are intended to be modified by users to enforce relaxed, cautious, and strict security policies in enterprises that include mixes of clients, servers, and applications that cannot be anticipated by ESM developers.

Best practice policies are preconfigured by members of the Symantec Security Response team to harden specific operating system platforms and protect known combinations of applications and OS platforms. These policies use preconfigured values, name lists, templates, and word files that directly apply to the targeted applications and platforms.

Best practice policies use the modules and templates from ESM Security Update releases to check OS patches, password settings, and other vulnerabilities on the targeted operating system. Best practice policies may also introduce new, application-specific modules and templates to check conditions that are specifically related to the targeted application and OS platform.

ESM best practice policies represent the collective wisdom of security experts, and they should not be modified by ESM users. In ESM 5.5, they are installed as read-only policies that cannot be edited by ESM users.

Warning: Do not attempt to modify an ESM best practice policy. Instead, copy and rename the policy, then edit the new version. This preserves the original best practice policy and also protects your customized policy from being overwritten by policy updates to the best practice policy.

How base policies differ from high-level policies

ESM best practice policies are configured as base policies, as high-level policies, or as sets that include both base and high-level policies.

Base policies are configured using the 80-20 rule of security. The 80-20 rule states that 80 percent of a successful compromise comes from 20 percent of a system's vulnerabilities or misconfiguration.

To detect critical system vulnerabilities, base policies are configured to:

- Identify unneeded services
- Identify missing OS patches
- Enforce password strength rules
- Check for application or platform-specific vulnerabilities that are deemed most critical by security experts

High-level policies incorporate checks for additional best practices that are prescribed by the ISO 17799 standard and recommended for specific application and OS platform combinations by trusted information security experts.

Industry research sources

Many of the security vulnerabilities that are addressed by the ISO 17799 standard and ESM best practice policies have been researched by industry security experts. Best practice recommendations that result from this research are posted to numerous Web sites and published as advisories by a variety of organizations that act as security information clearing houses.

Research resources for ESM best practice policies include, but are not limited to, the following:

- Symantec Security Response team
- CERT Coordination Center
- SANS Institute
- Computer Incident Advisory Center (CIAC)
- Center for Internet Security (CIS)
- National Infrastructure Protection Center (NIPC)
- National Security Agency (NSA)
- Information Systems Audit and Control Association (ISACA)
- Application and operating system vendors

Note: ESM best practice policies were researched using information that was released into the public domain by the organizations listed above. Recognition of these organizations does not indicate official endorsement of ESM best practice policies by any of these organizations.

Installing best practice policies

ESM best practice policies should be installed on the ESM managers that will run the policies on ESM agents with the applications and/or operating system platforms that are targeted by the policies.

Installation prerequisites

Before you run the executable program that installs the best practice policy that is documented in this manual, you need to complete the following prerequisites:

- Upgrade all ESM manager and agent systems that will use the best practice policies to ESM version 5.1 or later.
- Upgrade the UNIX modules on all ESM manager and agent systems that will use the best practice policies to Security Update 9 or later.
- Download the **BestPractice_AIX_4x_UNIX_ISO** executable file on the Symantec Security Response Web site at:

  http://securityresponse.symantec.com
- Identify the ESM account name, the ESM account password, and the communication port that you will need to connect to each ESM manager you intend to install.

Installation steps

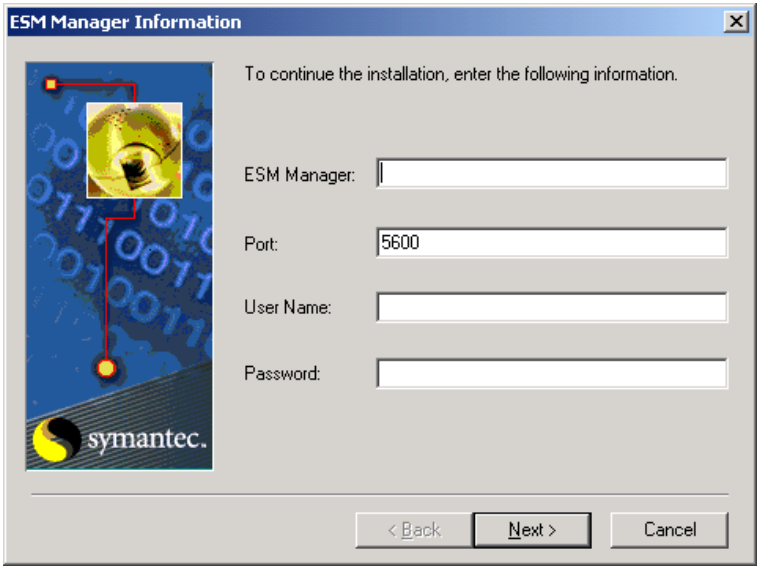
1. Run the **BestPractice_AIX_4x_UNIX_ISO** executable file from a Windows NT, Windows 2000, or Windows XP system that has network access to the ESM manager you want to install.
2. Click **Next** to close the InstallShield Welcome dialog box.
3. Click **Yes** to accept the Symantec Corporation Software License Agreement.

Warning: If the install program does not find the required Java™ 2 Runtime Environment on your system, the program returns an error and aborts the installation. Download and install the Java 2 Runtime Environment, then rerun the install program.

---

4. Click **Yes** to continue installation of the best practice policies.

5 Enter requested ESM manager information, then click **Next**.



Note: The install program returns an error message and aborts the installation when it does not find an agent with the required operating system platform nor all of the modules that are executed by the policy on the specified manager. Register an agent with the required operating system and install the latest security update, then rerun the install program.

6 Click **Finish** to exit the install program after a successful installation.

AIX base policy

The AIX base policy runs the following ESM security checks on AIX operating system to enforce ISO 17799 standard-based best practices. See the *ESM Security Update User's Guide for UNIX Modules* for more information about the security checks and templates that are enabled in the documented policy.

OS Patches checks and templates

Make sure that all patches that are defined in the AIX patch.pai template file are installed on applicable versions of AIX operating systems. See ISO 17799 section 10.4.1.

Note: Make sure that you are using the patch.pai template file that was installed by ESM Security Update 9 or later. If you have edited this template, you should restore it to its previous state.

Password Strength checks

- **Password = username**, **Password = any username**, **Password Within GECOS Field**, and **Password = wordlist word**. Passwords that are used to log in to your AIX systems should not match any user name on your system, any name in GECOS fields in the /etc/passwd file, or any commonly-used dictionary word. The AIX base policy checks all passwords against both upper and lowercase forms of user names and word list words and reports user accounts that require password changes. See ISO 17799 section 9.3.1(d)(2).
- **Login requires password** and **Accounts without passwords**. Require passwords to log in to all user accounts. See ISO 17799 sections 9.3.1 and 9.5.3.
- **Check password length restrictions**. Require passwords of at least six characters. See ISO 17799 section 9.3.1(d).

Startup Files checks and templates

- **Services**. The AIX base policy checks your AIX operating systems for services that are defined in the aix4xb.sai Services template file. Install any Mandatory services that are reported as missing and remove any installed services that are reported as Forbidden. See ISO 17799 sections 8.3, 9.4.1, and 9.4.9.
- **Report Services not in template**. Review all system-owned processes that are reported by this check, but not listed in the Services template. Remove all unnecessary services from ESM agents. See ISO 17799 sections 8.3, 9.4.1, and 9.4.9.

AIX high-level policy

The AIX high-level policy runs all of the security checks that are included in the base policy as well as the following checks to ensure compliance with ISO 17799 standard-based best practices. See the *ESM Security Update User's Guide for UNIX Modules* for more information about the security checks and templates that are enabled in the documented policy.

Account Integrity checks

- **Illegal login shells** and **Nonexistent login shells.** Ensure that all user accounts have login shells that are listed in the /etc/shells file. See ISO 17799 section 9.6.1.(a) and (b).
- **Setuid login shells** and **Setgid login shells.** Remove setuid and setgid privileges from login shells. Executable files that run as the file owner or group owner may provide unauthorized access to other files on your systems. See ISO 17799 sections 9.5.3, 9.5.5 (c), and 9.6.1 (c).
- **Home directory permissions.** Enforce secure home directory permissions of at least 750. See ISO 17799 section 9.1.1.2 (b).
- **Changed accounts** and **Changed groups.** Review all user accounts and groups that have changed since the user or group snapshot file was last updated. If reported accounts were not changed by the system administrator, they may represent a security breach. See ISO 17799 section 9.2.4 (c).

Note: The Account Integrity module creates and maintains an agent snapshot file that stores information about user accounts on the system. Run the module one time to create the snapshot. Then periodically rerun the policies to detect service changes.

- **Duplicate IDs.** Remove or disable user IDs (UIDs) and group IDs (GIDs) that are shared by two or more users or groups. See ISO 17799 sections 9.2.1 (a) and 9.5.3.
- **Privileged users and groups.** Remove or disable users and groups that have a user ID or group ID that allows super-user privileges or privileged access to system files. See ISO 17799 section 9.2.2 (e).
- **Accounts that must be disabled.** Disable unauthorized user accounts.
- **Password in /etc/passwd.** Remove or disable users with passwords that are contained in the /etc/passwd file when the system is using, or has access to, shadow files or enhanced security files. See ISO 17799 section 9.2.3.

File Attributes checks

- **Check file user ownership, Check file group ownership,** and **Check file permissions.** Enforce the file user ownership, file group ownership, and file permission values that are specified in the aix4xh.aix template file. See ISO 17799 sections 9.5.5 (a, c, g) and 9.6.1 (c).

  Note: The File Attributes module creates and maintains an agent snapshot file that stores information about files on the system. Run the module one time to create the snapshot. Then periodically rerun the policies to detect service changes.

- **Check file creation time, Check file modification time,** and **Check file size.** Files that are specified in the template file should have the same file creation times, modification times, and file sizes that are stored in the agent's snapshot file. See ISO 17799 section 10.4.1 (a).
- **Perform checksum check (CRC/MD5).** This check detects changes to files by comparing file checksums with the checksums in the most recent snapshot files.

  Comparing file checksums is superior to comparing creation time, modification time, and file size because it is significantly more difficult for someone to change a checksum without detection. See ISO 17799 section 10.4.1 (a).

File Find checks

- **Setuid files, Setgid files, New setuid files,** and **New setgid files.** Remove the setuid and setgid attribute from unauthorized files.

  Anyone running a setuid or setgid file is temporarily assigned the user ID of the file. While many system files depend on this attribute for proper operation, security problems can result if setuid or setgid is assigned to programs that allow reading and writing of files or escapes to shell. See ISO 17799 section 9.2.2.

- **World writable files.** Reassign permissions to files that are writable by everyone. World writable files are security risks because there are no controls over who can modify or delete these files. See ISO 17799 section 9.1.1.2 (b).

- **Uneven file permissions.** Reassign permissions on files with other access that is greater than group access or user access. Also, reassign permissions on files with group access that is greater that user access. A file with uneven permissions is inconsistent and does not make sense from a security perspective. See ISO 17799 section 9.1.1.2 (b).

- **Unowned directories/files.** Remove or change the owner of directories or files with ownerships (UID or GID) that cannot be associated with user or group names on the system being checked. These files are not accounted for and do not make sense from a security perspective. See ISO 17799 section 9.2.1 (h).

File Watch checks

- **Enable ownership checks.** Examine files and directories in the /bin, /lib, /sbin, /usr/bin, /usr/lib, and /usr/sbin directories for ownership changes. Run the module first to create the snapshot file. Then examine the results of ongoing checks to make sure changes were authorized. See ISO 17799 sections 9.5.5.9 (a, c, g) and 9.6.1 (c).
- **Enable permissions checks.** Examine files and directories in the /bin, /lib, /sbin, /usr/bin, /usr/lib, and /usr/sbin directories for recently modified or expanded permissions. Run the module first to create the snapshot file. Then examine the results of ongoing checks to make sure changes were authorized. See ISO 17799 section sections 9.5.5.9 (a, c, g) and 9.6.1 (c).
- **Enable signature checks (against snapshot).** Calculate MD5 and CRC signatures on files and directories in the /bin, /lib, /sbin, /usr/bin, /usr/lib, and /usr/sbin directories and compare the results with signatures that are stored in the agent's snapshot file. Run the module first to create the snapshot file. Then examine the results of ongoing checks to make sure changes were authorized. See ISO 17799 section 10.4.1 (a).
- **Enable new file checks.** Examine recently created files and directories in the /bin, /lib, /sbin, /usr/bin, /usr/lib, and /usr/sbin directories. See ISO 17799 section 10.4.1 (a).
- **Enable removed file checks.** Examine recently removed files and directories in the /bin, /lib, /sbin, /usr/bin, /usr/lib, and /usr/sbin directories. See ISO 17799 section 10.4.1 (a).

Login Parameters checks

- **Inactive accounts.** Remove or disable accounts that have never been logged into and accounts that have not been logged into during the previous 30 days. See ISO 17799 section 9.2.1 (h).
- **Login failures.** Examine user accounts with an unusual number of failed login attempts during the previous 15 days. See ISO 17799 sections 9.5 (b) and 9.7.1 (d).
- **Remote root logins.** Prevent root access through rlogin and telnet. The root account should be accessed only through the system console. See ISO 17799 section 9.5.1.

Network Integrity checks

- **NFS exported dirs with no access lists.** Use access lists with NFS exported directories to limit access to intended users. Without access lists, exported directories allow world access. See ISO 17799 section sections 9.4.1, 9.4.3, 9.6.1, and 9.1.1.2 (b).
- **NFS exported dirs with anonymous access.** Prevent anonymous users from accessing NFS exported directories. See ISO 17799 sections 9.4.1 and 9.4.3.

Password Strength checks

- **System/user max password age.** Require password changes at least every 60 days. Frequent password changes increase the overall security of the system. You should require users to change their passwords periodically (at least one time each 60 days). See ISO 17799 section 9.3.1 (e).

Startup Files checks

- **Report duplicate services.** Examine all system-owned services, processes, or commands that are duplicated on the system (i.e., found in the process table more than once) and decide if any should be removed or disabled. This includes system-owned commands that are running multiple times in the process table. See ISO 17799 sections 8.3, 9.4.1, and 9.4.9.
- **Changed services** and **New services.** First run the module to create a snapshot. Then examine services that have been added or with configurations that have been changed since the last time the ESM service snapshot was updated. See HIPAA sections 8.3, 9.4.1, and 9.4.9.

User Files checks

- **File ownership.** Reassign permissions to user files and directories that have different UIDs or GIDs than the IDs listed in the agent's password file. Incorrect file ownership can allow unauthorized access to files or prevent authorized users from accessing the files.
- **World writable files.** Reassign permissions to user files and directories that are world writable. Files that are writable by everyone represent a security risk because there are no controls to restrict who can modify or delete these files. See ISO 17799 section 9.1.1.2 (b).
- **Set UID or GID.** Remove the set user ID (setuid) or the set group ID (setgid) from unauthorized files. Files that set the UID or GID of users executing the files to the UID or GID of the file owner, or to other users, may allow unauthorized access to other files. See ISO 17799 section 9.2.2.
- **Check startup file contents.** Examine startup files for security risks. For users with .rhosts files, the check produces a list of users and systems that are not required to enter a password. For users with .netrc files, the check produces a list of entries containing passwords. See ISO 17799 sections 9.4.3, 9.3.1 (g), and 9.2.3.
- **Check startup file protection.** Ensure proper ownerships and permissions for the .cshrc, .exrc, .forward, .login, .mailrc, .netrc, .newsrc, .nodes, .profile, .rhosts, and .Xdefaults files.
- **Suspicious file names.** Examine executable files with "suspicious" names in the user's home directory tree. A suspicious name is one that is the same as a user name or the name of a system command listed in the man pages. An executable with a suspicious name can be executed unknowingly by another user. This can occur when a common user or system command is input and the path is not set up properly. See ISO 17799 section 8.3.
- **Device files.** Examine block-special and character-special (device) files in the user's home directory tree. See ISO 17799 section 9.2.2.
- **Mount points.** Examine mount points within the user's home directory tree. It is not standard practice to mount devices in user areas. This can represent unauthorized access to data on the device in question. See ISO 17799 section 9.2.2.

Known restrictions

Registration of new agents to ESM 5.1 managers

When you register an ESM 5.1 agent with an operating system that was not registered to your ESM 5.1 manager before you installed a best practice policy, the new agent's operating system inaccurately displays in the policy's expanded module lists in the ESM enterprise tree.

For example, if you install the AIX base policy on an ESM 5.1 manager where only UNIX agents are registered, then register a Windows 2000 agent to that manager, the WIN2000 agent listing displays in the module lists. This is misleading, because this policy does not run on Windows 2000 agents. Reinstall the policy to correct the module listings.

These are cosmetic errors that are fixed in the ESM 5.5 console release. If you are using the ESM 5.1 console, remember that each ESM best practice policy is intended to run only on ESM agents that are running the applications and/or operating system versions that are targeted by the policy.

Service and support solutions

You can reach Customer Service and Technical Support for Symantec Enterprise Security Manager and add-on products on the Internet or by telephone.

This chapter includes the following topics:

- Before contacting technical support
- Service and support Web site
- Service and support offices

Before contacting technical support

Before contacting technical support

1. Use online Help to look up the information you need.
2. Read the relevant portions of this guide and your *Symantec Enterprise Security Manager User Manual*. This guide is available as a PDF file on the product CD.
3. Consult the Symantec ESM Release Notes for the version that you are using at http://securityresponse.symantec.com.
4. Gather the following information:

Category	Information	Source
Console	Machine type	Windows: System properties
	OS level	System properties

Category	Information	Source
	Version	**Help** > **About**
	Date	**Help** > **About**
Manager	Machine type	UNIX: **uname -a** NT/2000: System properties
	OS level	UNIX: **uname -a** NT/2000: System properties NetWare: Version command
	Version and date	Manager properties
Agent	Machine type	UNIX: **uname -a** NT/2000: System properties NetWare: Version command
	OS level	UNIX: **uname -a** NT/2000: System properties NetWare: Version command
	Version and date	Agent properties
Network	Protocol vendor and version	
Problem	Symptoms	
	Steps to reproduce	
	Error message text (all characters)	
	System log file text	

Service and support Web site

The award-winning Symantec Service and Support Web site provides a wide variety of methods to help you solve your enterprise technical issues. Point your browser at http://www.symantec.com/techsupp/.

Knowledge Base

Search the Symantec Enterprise Security Manager Knowledge Base to find answers to common problems and questions. The Symantec Knowledge Base contains 90 percent of all known issues with accompanying solutions.

Often this is the fastest way to get the information that you are looking for.

If you do not use Microsoft Internet Explorer, you may have to go first to http://www.msn.com, then to http://www.symantec.com/techsupp/

LiveUpdate for databases, firewalls, and Web servers

Systems that are installed with manager and agent software can also be upgraded with SU9 and later Security Update releases through Symantec's LiveUpdate technology.

Download updated modules for Symantec ESM for databases, firewalls, and Web servers. Symantec ESM 5.5 and a subscription to LiveUpdate are required. See the *Symantec Enterprise Security Manager 5.5 User Manual*.

Releases and updates

Download new products and Security Updates using LiveUpdate or from the Symantec Security Response Web site at http://securityresponse.symantec.com.

Manuals and documentation

Download current user's guides, installation guides, and other documentation in PDF format. Most PDF documents can be found on the product CD.

Web support

Log questions or problems for Technical Support. You can also create a case, add notes to a case, check the status of a case, and close a case.

Email support

Email pre-sales or non-technical questions to Customer Service for service options.

Symantec ESM news bulletins

Subscribe to this product specific mailing list for:

- Up-to-date notification of product upgrades
- Latest offerings from Technical Support
- Product tips and tricks

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.service.symantec.com/mx
+54 (11) 5382-3802

Asia/Pacific Ring

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.service.symantec.com/mx
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

http://www.service.symantec.com/mx

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

June 2002